UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/735,992	12/15/2003	Amer Hassan	M1103.70182US00	2966

45840 7590 03/09/2007

WOLF GREENFIELD (Microsoft Corporation)
C/O WOLF, GREENFIELD & SACKS, P.C.
FEDERAL RESERVE PLAZA
600 ATLANTIC AVENUE
BOSTON, MA 02210-2206

EXAMINER	
GELAGAY, SHEWAYE	
ART UNIT	**PAPER NUMBER**
2137	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/09/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/735,992	HASSAN ET AL.	
	Examiner	Art Unit	
	Shewaye Gelagay	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 December 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19 and 25-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19 and 25-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *6/1/05,5/17/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Election/Restrictions

1. Restriction to one of the following inventions is required under 35 U.S.C. 121:

I. Claims 1-19 and 25-33, drawn to method of wirelessly generating a cryptographic key by modulating signal, classified in class 380, subclass 31.

II. Claims 20-24 and 34-42, drawn to method of wireless communication between two devices, classified in class 713, subclass 171.

2. The inventions are distinct, each from the other because of the following reasons:

Inventions Group I and Group II are related as combination and subcombination. Inventions in this relationship are distinct if it can be shown that (1) the combination as claimed does not require the particulars of the subcombination as claimed for patentability, and (2) that the subcombination has utility by itself or in other combinations (MPEP § 806.05(c)). In the instant case, the combination as claimed does not require the particulars of the subcombination as claimed because Group I is a method of generating key and Group II is a method of wireless communication between two devices. The subcombination has separate utility such as key generation.

The examiner has required restriction between combination and subcombination inventions. Where applicant elects a subcombination, and claims thereto are subsequently found allowable, any claim(s) depending from or otherwise requiring all the limitations of the allowable subcombination will be examined for patentability in accordance with 37 CFR 1.104. See MPEP § 821.04(a). Applicant is advised that if any claim presented in a continuation or divisional application is anticipated by, or includes all the limitations of, a claim that is allowable in the present application, such claim may be subject to provisional statutory and/or nonstatutory double patenting rejections over the claims of the instant application.

Because these inventions are independent or distinct for the reasons given above and there would be a serious burden on the examiner if restriction is not required because the inventions have acquired a separate status in the art in view of their different classification, restriction for examination purposes as indicated is proper.

Because these inventions are independent or distinct for the reasons given above and there would be a serious burden on the examiner if restriction is not required because the inventions require a different field of search (see MPEP § 808.02), restriction for examination purposes as indicated is proper.

3. During a telephone conversation with James Morris (Tel. 617-646-8227) on 2/26/07 a provisional election was made without traverse to prosecute the invention of Group I, claims 1-19 and 25-33. Affirmation of this election must be made by applicant in replying to this Office action. Claims 20-24 and 34-42 are

withdrawn from further consideration by the examiner, 37 CFR 1.142(b), as being drawn to a non-elected invention.

4. Applicant is reminded that upon the cancellation of claims to a non-elected invention, the inventorship must be amended in compliance with 37 CFR 1.48(b) if one or more of the currently named inventors is no longer an inventor of at least one claim remaining in the application. Any amendment of inventorship must be accompanied by a request under 37 CFR 1.48(b) and by the fee required under 37 CFR 1.17(i).

Claim Rejections - 35 USC § 101

5. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. Claim 25 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim 25 is directed towards a computer program product on computer readable medium wherein the computer readable medium is not defined by the specification as being a storage medium. Applicant's specification discloses, "Computer readable media may include a communication media . . .data in a modulated data signal such as carrier wave .. ." (page 8, paragraph 25) but does not specifically mention that the downloaded program product is stored in a storage medium. Examiner further suggests amending the claim limitation to specify that the computer operable media is a storage medium.

7. Claims 26-33 are also rejected for being dependent on a rejected claim.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1-19 and 25-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Abe et al. (hereinafter Abe) US Publication Number 2005/0123138 in view of Diffie et al. (hereinafter Diffie) US Patent Number 5,371,794.

As per claims 1, 10 and 25:

Abe teaches a method of wirelessly generating a cryptographic key that may be used to encrypt wireless communications between a first host and a second host, the method comprising the steps of:

selecting an initial modulation scheme for wireless transmission between the first host and the second host; (page 4, paragraphs 102-105; page 7, paragraphs 149-150)

transmitting via the initial modulation scheme first data to be used in generating the cryptographic key; (page 4, paragraphs 106-108; page 7, paragraph 149-page 8, paragraph 151)

receiving via the second modulation scheme second data to be used in generating the cryptographic key; (page 5, paragraph 109-111; page 8, paragraphs 152-154)

generating the cryptographic key using the first and the second data. (page 5, pargraphs 112-115; page 8; paragraphs 158-163)

Abe does not explicitly initial modulation scheme with an indication of a second modulation scheme. Diffie in analogous art, however, discloses initial modulation scheme with an indication of a second modulation scheme. (col. 8, line 43-col. 9, line7) Therefore it would have been obvious to one ordinary skill in the art to modify the method disclosed by Abe with Diffie in order to provide a system that prevents key change messages from being played back, without resort to sequence numbers. (col. 10, lines 65-67; Diffie)

As per claims 2, 11 and 26:

The combination of Abe and Diffie teaches all the subject matter as discussed above. In addition, Abe further discloses a method wherein the step of receiving further comprises the step of receiving via the second modulation scheme an indication of a third modulation scheme, the method further comprising the steps of:

transmitting via the third modulation scheme third data to be used in generating the cryptographic key and an indication of a fourth modulation scheme; (page 10, paragraphs 193-195;)

receiving via the fourth modulation scheme fourth data to be used in generating the cryptographic key; (page 11, paragraphs 196-198) and

wherein the step of generating the cryptographic key using the first and the second data further comprises the step of generating the cryptographic key using the first, second, third, and fourth data. (page 11, paragraph 199-page 12, paragraph 219)

As per claim 3, 14, 19 and 27:

The combination of Abe and Diffie teaches all the subject matter as discussed above. In addition, Abe further discloses a method comprising the steps of:

determining a desired modulation scheme for wireless communications between the first host and the second host; (page 4, paragraphs 102-105; page 7, paragraphs 149-150)

encrypting wireless data to be transmitted using the cryptographic key; (page 11, paragraph 199-page 12, paragraph 219) and

transmitting the encrypted wireless data via the desired modulation scheme. (page 11, paragraph 199-page 12, paragraph 219)

As per claim 4, 13 and 28:

The combination of Abe and Diffie teaches all the subject matter as discussed above. In addition, Abe further discloses determining a size of the cryptographic key; (page 11, paragraph 199-page 12, paragraph 219) and monitoring an amount of data exchanged; (page 11, paragraph 199-page 12, paragraph 219) In addition, Diffie further discloses selecting a final modulation scheme for a final data exchange between the first host and the second host such that an amount of data conveyed by the final modulation scheme added to

the amount of data exchanged equals the size of the cryptographic key. (col. 10, lines 42-46)

As per claim 5, 16 and 29:

The combination of Abe and Diffie teaches all the subject matter as discussed above. In addition, Diffie further discloses wherein the step of selecting an initial modulation scheme comprises the step of sharing a short key established by a public key method, the short key providing an index to the initial modulation scheme. (col. 10, lines 25-41)

As per claim 6, 17 and 30:

The combination of Abe and Diffie teaches all the subject matter as discussed above. In addition, Diffie further discloses wherein the step of sharing a short key established by a public key method comprises the step of sharing a short key established by a Diffie-Hellman key exchange method. (col. 10, lines 25-41)

As per claim 7 and 31:

The combination of Abe and Diffie teaches all the subject matter as discussed above. In addition, Diffie further discloses a key exchange method of sending and receiving messages in a wireless network using certificate digitally signed by a certificate authority. It would have been obvious to one ordinary skill in the art at the time the invention was made to modify the method disclosed by Abe and Diffie to include wherein the step of sharing a short key established by a public key method comprises the step of sharing a short key established using Kerberos in order to have a system that prevents key change messages from

being played back, without resort to sequence numbers. (col. 10, lines 65-67; Diffie)

As per claim 8, 18 and 32:

The combination of Abe and Diffie teaches all the subject matter as discussed above. In addition, Abe further discloses wherein the step of selecting an initial modulation scheme comprises the step of selecting an initial constellation. (page 4, paragraphs 102-105; page 7, paragraphs 149-150)

As per claims 9 and 33:

The combination of Abe and Diffie teaches all the subject matter as discussed above. In addition, Abe further discloses wherein the step of selecting an initial modulation scheme comprises the step of selecting an initial bit assignment for a constellation.

As per claim 12 and 15:

The combination of Abe and Diffie teaches all the subject matter as discussed above. In addition, Abe further discloses comprising the steps of: receiving modulated information; and demodulating the modulated information via the next modulation scheme to extract the data. (page 5, pargraphs 112-115; page 8; paragraphs 158-163)

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See Form PTO-892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shewaye Gelagay whose telephone number is 571-272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Shewaye Gelagay SG

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER